

2/13/2006

In the Claims

1  
2 Please cancel claims 1—82.  
3

4       ~~83.~~ (New) A method, at least partially implemented by a computer,  
5 comprising:  
6

7             building a data block comprising a first random value and a cryptographic  
8 hash of the first random value;

9             generating, on a second computing device, a signature by digitally signing a  
10 string containing a second random value; and

11             computing an encryption key, for encrypting the data block, by hashing a  
12 combination of the signature and a third random value.

13       ~~2~~ ~~84.~~ (New) The method as recited in Claim ~~83~~, wherein the second  
14 computing device is a smart card.

15       ~~3~~ ~~85.~~ (New) The method as recited in Claim ~~83~~, wherein the combination  
16 of the digitally signed string and the third random value comprises the digitally  
17 signed string concatenated to the third random value.

18       ~~4~~ ~~86.~~ (New) The method as recited in Claim ~~83~~, wherein the combination  
19 of the digitally signed string and the third random value comprises the third  
20 random value concatenated to the digitally signed string.

1           ~~5~~ 87. (New) The method as recited in Claim ~~83~~, further comprising:

2           encrypting the data block using the encryption key; and

3           storing the encrypted data block and the second and third random values.

4           ~~6~~ 88. (New) The method as recited in Claim ~~87~~, further comprising:

5           accessing the stored encrypted data block and the second and third random  
6           values;

7           providing a string containing the second random value to the second  
8           computing device; and

9           generating, on the second computing device, a second signature by digitally  
10          signing the string containing the second random value.

12           ~~7~~ 89. (New) The method as recited in Claim ~~88~~, further comprising:

13           computing a decryption key using the second signature and the third  
14          random value;

15           decrypting the encrypted data block with the decryption key; and

16           comparing the decryption of the encrypted data block to the data block.

18           ~~8~~ 90. (New) The method as recited in Claim ~~89~~, wherein computing the  
19          decryption key comprises:

20           hashing the second signature concatenated to the third random value.

1      | 91. (New) The method as recited in Claim ~~89~~, further comprising:  
2                hashing the first random value contained within the decryption of the  
3                encrypted data block; and

4                comparing the result of this hash with the hash of the first random value  
5                contained within the decryption of the encrypted data block.

6      | 92. (New) A method, at least partially implemented by a computer,  
7                comprising:

8                accessing an encrypted data block, wherein the encrypted data block  
9                comprises an encryption of a combination of a first random value and a hash of the  
10                first random value;

11                accessing second and third random values;

12                providing a string containing the second random value to a second  
13                computing device;

14                generating, on the second computing device, a signature by digitally  
15                signing the string containing the second random value; and

16                computing a decryption key, configured to decrypt the encrypted data  
17                block, wherein computing the decryption key uses the signature generated on the  
18                second computing device and the third random value.

19      | 93. (New) The method as recited in Claim ~~92~~, wherein the second  
20                computing device is a smart card.  
21  
22  
23  
24  
25

~~94.~~ (New) The method as recited in Claim ~~92~~, wherein computing the decryption key comprises:

3 hashing the signature concatenated to the third random value.

13  
95. (New) The method as recited in Claim 92, further comprising:

6       decrypting the encrypted data block with the decryption key, wherein the  
7       first random value and the hash of the first random value are recovered by the  
8       decryption; and

9 comparing the first random value and the hash of the first random value  
10 recovered from the decryption to a data block from which the encrypted data block  
11 was generated.

14 96. (New) The method as recited in Claim 95, further comprising:

14 hashing the first random value recovered from the decryption of the  
15 encrypted data block; and

6 comparing the result of this hash with the hash of the first random value  
7 recovered from the decryption of the encrypted data block.

1           15  
2        97. (New) One or more computer-readable media comprising computer-  
3 executable instructions for encryption-based authentication, the computer-  
4 executable instructions comprising instructions for:

5           building a data block comprising a first random value and a cryptographic  
6 hash of the first random value;

7           generating, on a second computing device, a signature by digitally signing a  
8 string containing a second random value; and

9           computing an encryption key, for encrypting the data block, by hashing a  
10 combination of the signature and a third random value.

11          16  
12        98. (New) The one or more computer-readable media as recited in Claim  
13        15  
14        97, wherein the second computing device is a smart card.

15          17  
16        99. (New) The one or more computer-readable media as recited in Claim  
17        15  
18        97, wherein the combination of the digitally signed string and the third random  
19        value comprises the digitally signed string concatenated to the third random value.

20          18  
21        100. (New) The one or more computer-readable media as recited in Claim  
22        15  
23        97, wherein the combination of the digitally signed string and the third random  
24        value comprises the third random value concatenated to the digitally signed string.

19

1 101. (New) The one or more computer-readable media as recited in Claim  
2 97, further comprising instructions for:

3 encrypting the data block using the encryption key; and

4 storing the encrypted data block and the second and third random values.

20

5 102. (New) The one or more computer-readable media as recited in Claim  
6 101, further comprising instructions for:

7 accessing the stored encrypted data block and the second and third random  
8 values;

9 providing a string containing the second random value to the second  
10 computing device; and

11 generating, on the second computing device, a second signature by digitally  
12 signing the string containing the second random value.

21

13 103. (New) The one or more computer-readable media as recited in Claim  
14 102, further comprising instructions for:

15 computing a decryption key using the second signature and the third  
16 random value;

17 decrypting the encrypted data block with the decryption key; and

18 comparing the decryption of the encrypted data block to the data block.

21

22

23

24

25

1                   22  
21                 104. (New) The one or more computer-readable media as recited in Claim  
2                 103, wherein computing the decryption key comprises instructions for:

3                 hashing the second signature concatenated to the third random value.

4                   23  
5                 21                 105. (New) The one or more computer-readable media as recited in Claim  
6                 103, further comprising instructions for:

7                 hashing the first random value contained within the decryption of the  
8                 encrypted data block; and

9                 comparing the result of this hash with the hash of the first random value  
10                 contained within the decryption of the encrypted data block.

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

24

1 106. (New) One or more computer-readable media comprising computer-  
2 executable instructions for encryption-based authentication, the computer-  
3 executable instructions comprising instructions for:

4 accessing an encrypted data block, wherein the encrypted data block  
5 comprises an encryption of a combination of a first random value and a hash of the  
6 first random value;

7 accessing second and third random values;

8 providing a string containing the second random value to a second  
9 computing device;

10 generating, on the second computing device, a signature by digitally  
11 signing the string containing the second random value; and

12 computing a decryption key, configured to decrypt the encrypted data  
13 block, wherein computing the decryption key uses the signature generated on the  
14 second computing device and the third random value.

15 25

16 107. (New) The one or more computer-readable media as recited in Claim  
17 106, wherein the second computing device is a smart card.

18 26

19 108. (New) The one or more computer-readable media as recited in Claim  
20 106, wherein computing the decryption key comprises instructions for:

21 hashing the signature concatenated to the third random value.

1                   27  
109. (New) The one or more computer-readable media as recited in Claim  
2                   24  
106, further comprising instructions for:

3                   decrypting the encrypted data block with the decryption key, wherein the  
4                   first random value and the hash of the first random value are recovered by the  
5                   decryption; and

6                   comparing the first random value and the hash of the first random value  
7                   recovered from the decryption to a data block from which the encrypted data block  
8                   was generated.

9                   28  
109. (New) The one or more computer-readable media as recited in Claim  
27  
109, further comprising instructions for:

12                  hashing the first random value recovered from the decryption of the  
13                  encrypted data block; and

14                  comparing the result of this hash with the hash of the first random value  
15                  recovered from the decryption of the encrypted data block.

16                  29  
111. (New) A system configured for encryption-based authentication,  
17  
18                  comprising:

19                  means for building a data block comprising a first random value and a  
20                  cryptographic hash of the first random value;

21                  means for generating, on a second computing device, a signature by  
22                  digitally signing a string containing a second random value; and

23                  means for computing an encryption key, for encrypting the data block, by  
24                  hashing a combination of the signature and a third random value.

30 29  
112. (New) The system as recited in Claim 111, wherein the second computing device is a smart card.

31 29  
113. (New) The system as recited in Claim 111, wherein the combination of the digitally signed string and the third random value comprises the digitally signed string concatenated to the third random value.

*32* *29*  
114. (New) The system as recited in Claim ~~111~~, wherein the combination of the digitally signed string and the third random value comprises the third random value concatenated to the digitally signed string.

*33*  
29 115. (New) The one or more computer-readable media as recited in Claim  
11 further comprising:

means for encrypting the data block using the encryption key; and  
means for storing the encrypted data block and the second and third random  
values.

34

- 1        116. (New) The system as recited in Claim 115, further comprising:  
2              means for accessing the stored encrypted data block and the second and  
3              third random values;  
4              means for providing a string containing the second random value to the  
5              second computing device; and  
6              means for generating, on the second computing device, a second signature  
7              by digitally signing the string containing the second random value.

35

- 8        35        34  
9        117. (New) The system as recited in Claim 116, further comprising:  
10              means for computing a decryption key using the second signature and the  
11              third random value;  
12              means for decrypting the encrypted data block with the decryption key; and  
13              means for comparing the decryption of the encrypted data block to the data  
14              block.

36

- 15        36        35  
16        118. (New) The system as recited in Claim 117, wherein computing the  
17              decryption key comprises:  
18              means for hashing the second signature concatenated to the third random  
19              value.

20  
21  
22  
23  
24  
25

37

1 119. (New) The system as recited in Claim 117, further comprising:  
2 means for hashing the first random value contained within the decryption of  
3 the encrypted data block; and  
4 means for comparing the result of this hash with the hash of the first  
5 random value contained within the decryption of the encrypted data block.

35

6 38  
7 120. (New) A system configured for encryption-based authentication,  
8 comprising:

9 means for accessing an encrypted data block, wherein the encrypted data  
10 block comprises an encryption of a combination of a first random value and a hash  
11 of the first random value;

12 means for accessing second and third random values;

13 means for providing a string containing the second random value to a  
14 second computing device;

15 means for generating, on the second computing device, a signature by  
16 digitally signing the string containing the second random value; and

17 means for computing a decryption key, configured to decrypt the encrypted  
18 data block, wherein computing the decryption key uses the signature generated on  
19 the second computing device and the third random value.

39

38

20 21 22 23 24 25 121. (New) The system media as recited in Claim 120, wherein the  
second computing device is a smart card.

1                          *40*                          *38*  
122. (New) The system as recited in Claim *120*, wherein computing the  
2 decryption key comprises:

3                          means for hashing the signature concatenated to the third random value.

4                          *41*                          *38*  
5                          123. (New) The system as recited in Claim *120*, further comprising:  
6                          means for decrypting the encrypted data block with the decryption key,  
7                          wherein the first random value and the hash of the first random value are  
8                          recovered by the decryption; and

9                          means for comparing the first random value and the hash of the first  
10                         random value recovered from the decryption to a data block from which the  
11                         encrypted data block was generated.

12                          *42*                          *41*  
13                          124. (New) The system as recited in Claim *123*, further comprising:

14                          means for hashing the first random value recovered from the decryption of  
15                         the encrypted data block; and

16                          means for comparing the result of this hash with the hash of the first  
17                         random value recovered from the decryption of the encrypted data block.

18  
19  
20  
21  
22  
23  
24  
25